VULNERABILITY REPORT

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/17/2021	A V Puneeth	Initial Version

TABLE OF CONTENTS

GENERAL INFORMATION

SCOPE

VIT-AP University has mandated us to perform security tests on the following scope:

- Software Security

ORGANISATION

The testing activities were performed between 05/17/2021 and 05/31/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-003	XSS	
High	IDX-001	Buffer Overflow	
Medium	VULN-002	Denial of Service	

TECHNICAL DETAILS

SHELL CODE INJECTION

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**8.2**
CVSSV3 CRITERIAS	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**Low**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE				
DESCRIPTION	Summary: Stored XSS can be submitted on reports, and anyone who will check the report the XSS will trigger. Description: Stored XSS, also known as persistent XSS, is the more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.			
OBSERVATION	Steps To Reproduce: I wanted test on this site https://app.mopub.com/reports/custom/ Now Click New network report. enter payload: "><img src=x onerror=alert(document.domain)> in the Click Run and save then XSS will trigger. Demonstration of the vulnerability: PoC: xssed.webm (F412243) Tested on Firefox and chrome.			
TEST DETAILS				
REMEDIATION	The attacker can steal data from whoever checks the report.			
REFERENCES				

BUFFER OVERFLOW

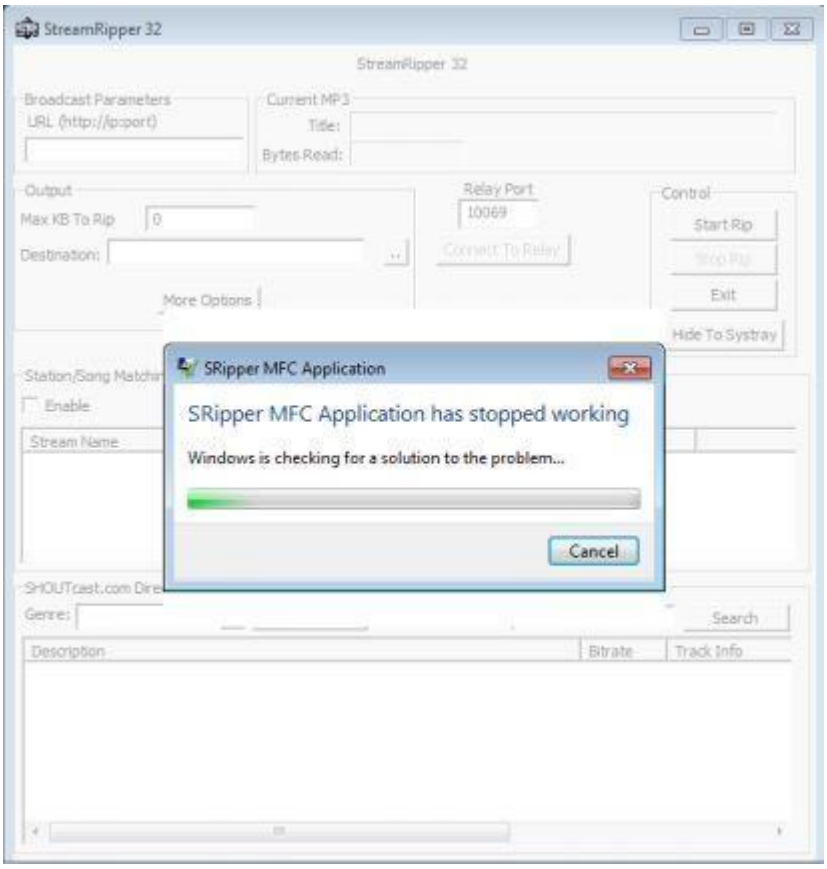
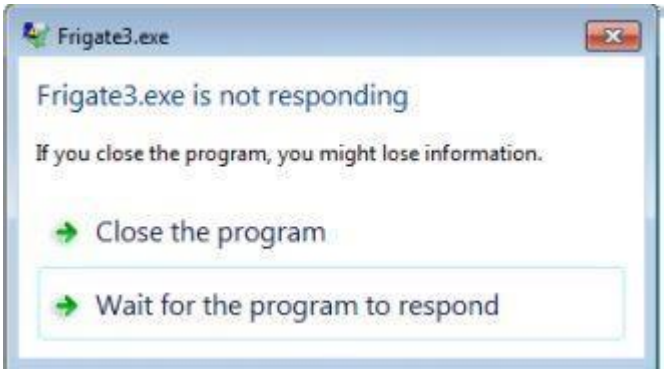
CVSS SEVERITY	High		CVSSV3 SCORE	7.6
CVSSV3 CRITERIAS	Attack Vector :	**Local**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**Low**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE				
DESCRIPTION	A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. It exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.			
OBSERVATION	We have observed that this buffer overflow can potentially crash an application and unknowingly allows command injection attacks.			
TEST DETAILS				

Image 1 – doc.JPG	
REMEDIATION	1. Address space randomization (ASLR) 2. Data execution prevention (DEP) 3. Structured exception handler overwrite protection (SEHOP)
REFERENCES	

DENIAL OF SERVICE

CVSS SEVERITY	Medium		CVSSV3 SCORE	5.5
CVSSV3 CRITERIAS	Attack Vector :	**Local**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**None**
	Required Privileges :	**None**	Integrity :	**None**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE				
DESCRIPTION	The Denial of Service (DoS) attack is focused on making an software unavailable for the purpose it was designed. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses. I			
OBSERVATION	We have observed that the software crashes immediately as a result of large string input due to Buffer overflow vulnerability. This could impact the availability of software			
TEST DETAILS	 Image 2 – buff.JPG			
REMEDIATION	!. Input Sanitization 2. Addressing Buffer Overflow			
REFERENCES				